FORTINET
TRAINING SERVICES

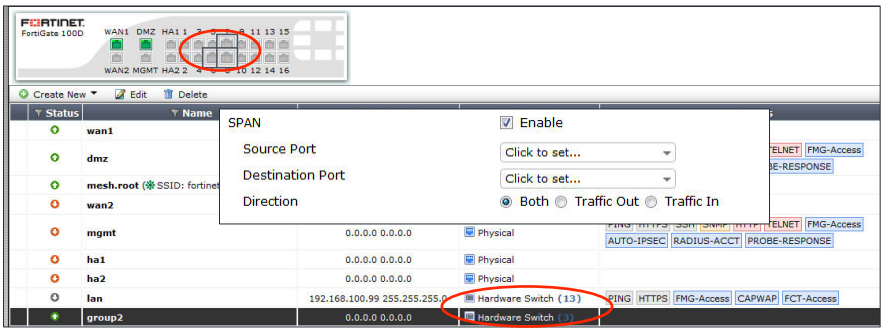
System: New Features & Changes

- Port Span
- FortiExtender
- Netflow v9.0
- FortiGuard with FortiManager
- LLDP Support
- Virtual Wan links
- Last Login time
- Combining Proxy and Flow based inspection

FORTINET

Port Span

- Also called 'Port Mirroring'
  - » Hardware Requirement: Hardware switch (100D, 140D, etc)
  - » Ingress &/or Egress traffic from a single port in a switch group can be copied to another port (in the same group)



3

Port Span: Deployment Scenario

- Customer needs to size their network for UTM and doesn't have the hardware to help figure it out
  - » Deploy Transparent FGT with no inspection of any kind
  - » Setup Port Spanning to mirror traffic
  - » Send traffic to a FGT
  - » Use One-Arm Sniffer mode to get a look at the traffic
- Network traffic can now be examined with no risk of disruption.
- Possible to use a single FGT instead of two
  - » If you loop the cable back to another port on the same FGT with Spanning, traffic could be inspected by the same device
  - » High CPU/Memory would still impact live traffic (possibly unsafe)

4

FortiExtender (FEX)

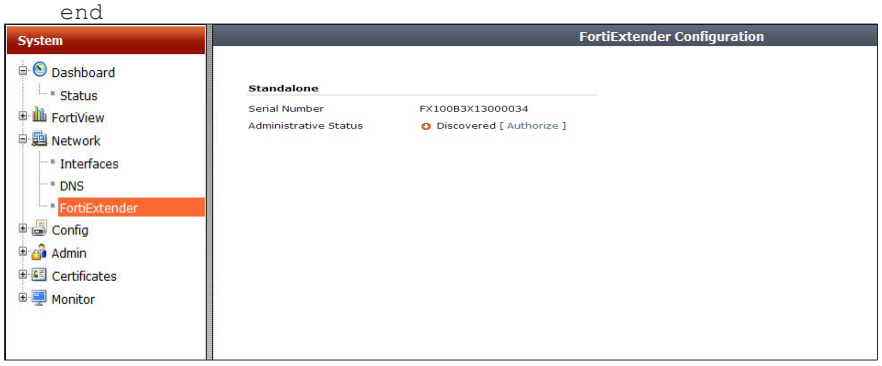
- Support added for FortiExtender
  - » a new product that turns a 4G/LTE modem into a Wifi network
  - » Some models require POE
  - » 20B (indoors)
  - » 100B (outdoors)
  - » 100A (outdoor w/ built-in mod
    - Verizon
  - » Managed via CAPWAP

5 FORTINET

FortiExtender: Configuration

- Enable in CLI

```
config sys global
     set fortiextender enable
end
```



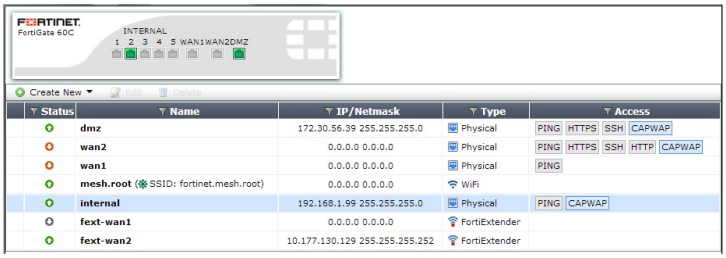
6 FORTINET

FortiExtender: Link status

- Links status can be either up or down
  - » indicates whether the CAPWAP tunnel between the Controller (FortiGate) and the FortiExtender is established or not

FortiExtender: Interfaces

- After authentication and modem dialup, information is on the System->Network->Interfaces page like a normal interface
  - » The IP/Netmask corresponds to the public IP the FortiExtender received from the ISP, and NOT the IP used by CAPWAP tunnel



Netflow: v9.0

- Netflow is a protocol published by Cisco
- Device Monitoring protocol that provides traffic information
- Different versions exist (1 thru 10)
  - » FortiGate only supports v9
  - » v10 is also known as IPFIX

9

Netflow: Configuration

- CLI

```
config system netflow
        set collector-ip <address>
        set collector-port <port>
        set source-ip <address>
        set active-flow-timeout <integer>
        set inactive-flow-timeout <integer>
end
```

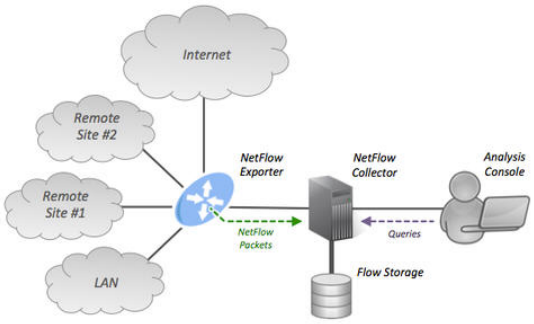
- Sampling is enabled per interface

```
config system interface
        edit <name>
        set netflow-sampler {disable | tx | rx | both}
        end
end
```

10

Netflow: Architecture

- FortiGate sends Netflow datagrams to configured collector
- Collector stores and reports are run based on data (like Syslog)
  - » Requires Netflow collector



11

Netflow: Design

- Operates as part of sflow process

```
diag test app sflowd ?

1. Show Sflow Collector Setting
2. Show Sflow Statistics
3. Show Netflow Collector Setting
4. Show Netflow Statistics
```

12

FortiGuard with FortiManager

- New port for FortiGuard WF & AS communications when connecting to a FortiManager (CLI Only)

```
#config system fortiguard
#set port ?
53      UDP Port 53 for server communication (for use by FortiGuard or FortiManager).
8888    UDP Port 8888 for server communication (for use by FortiGuard or FortiManager).
80      TCP Port 80 for server communication (for use only by FortiManager).
```

13

LLDP

Link Layer Description Protocol (LLDP) is a protocol defined IEEE 802.1AB which allows a device to advertise its existence/capabilities to other devices on a IEEE 802 LAN. It is documented in "802.1AB-2005 IEEE Station and Media Access Control Connectivity Discovery."

The primary purpose for adding LLDP is to improve the FortiGate device detection output when detecting another FortiGate device. Prior to this ECO there was very little that could be detected about a FortiGate since it does not generate a lot of traffic that uniquely identifies it. With the FortiGate now transmitting LLDP then that information is used to populate the device record on the FortiGate performing device detection. Because the FortiOS device detection feature is the primary user of the LLDP information then there are no explicit LLDP commands to display LLDP information about a peer device i.e. there is no equivalent of Cisco "show lldp". Any LLDP information transmitted by a peer is ignored unless FortiGate device detection is enabled on an interface. If device detection is enabled then the subset of LLDP information sent by the peer that is relevant to device detection is shown in the "diag user device list" output.

14

LLDP: Configuration

- Has 3 separate levels
- Global, per vdom, per interface.
  - » Most specific setting wins (Interface, Vdom, Global)
  - » Only available on interfaces with Static IPs

Global

```
config sys global
set lldp-transmission [enable|disable] ; default is enable
```

Vdom, per interface

```
config sys setting
set lldp-transmission [global|enable|disable] ; default is global
```

Interface

```
config sys interface
set lldp-transmission [vdom|enable|disable] ; default is vdom
```

15

LLDP: Information transmitted

Field	Contents
Chassis ID	The interface alias if defined, otherwise the interface name.
Port ID	The interface alias if defined, otherwise the interface name.
TTL	120 seconds
System Name	The FortiGate model e.g. "FortiGate-100D"
System Description	The same content as the Version in "get system status" e.g. "FortiGate-100D v5.2.0,build0526,140114 (Interim)"
System Capabilities	Indicates that the port can be part of a router or a bridge and whether it is part of a router/bridge based on whether the VDOM the port is a member of is in nat/ route mode or transparent mode
Aggregation	Indicates whether the port is a member of an aggregate and if so whether the aggregation was successful
Host Name	The hostname of the FortiGate. This s identical to the output of output of Hostname in "get system status". By default it would include the model and serial number e.g. "FG100D3G12804150". Since the serial number is a semi-private value, this field is not sent as plain text, rather it is encrypted with a key that is only known by Fortinet

16

LLDP Modified packet sniff

```
diag sniff packet wan1 ''

36.770744 arp who-has 172.16.67.206 tell 172.16.67.1
37.188606 lldp 160 chassis 6 'wan1' port 5 'wan1' ttl
120 system 'FortiGate-100D'
37.663858 arp who-has 172.16.67.100 tell 172.16.67.191
```

The only attributes used for device identification purposes are the System Name/Description and Host Name fields. The Chassis ID, Port ID and TTL are sent because they are mandatory in LLDP spec. The System Capabilities is sent because it is simple for FortiOS to provide. The Aggregation attribute is sent with the intent that it could be used to diagnose aggregation issues i.e. by looking at the LLDP attributes on a peer (e.g. Cisco) it would be possible to tell if the FortiGate ports were actually configured for aggregation.

LLDP CLI Commands

- LLDP does not generate log messages

```
diag debug application lldptx -1
```

- Enable debugs

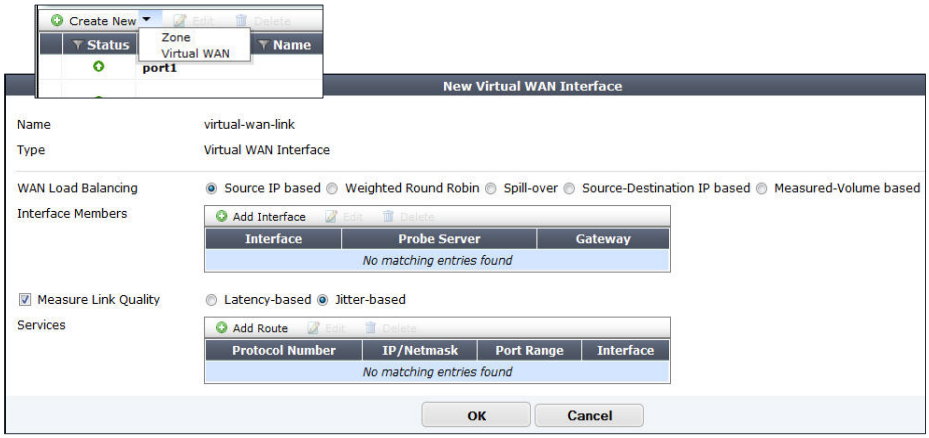
```
diag lldptx ?

stats              Source visibility statistics.
log                Debug log.
scheduler-times    Scheduler times.
restart            Restart LLDP transmitter.
```

Virtual Wan Link

- Previously multiple WAN links had to be configured as separate interfaces with duplicate firewall policies.
  - » Prone to policy errors
- Interfaces can be combined in a single logical interface even though each one will have a separate IP, Gateway and likely ISP
  - » Only 1 virtual WAN supported (per VDom)
  - » Configurable load balance/failover options

19

Virtual Wan Link: Configuration




```
#config sys virtual-wan-link
```

20

Virtual Wan Link: Load Balance Method

- Source IP - Source IP hashed
  - A source IP will always use the same WAN
- Weighted Round Robin
  - Session based weight (Identical to HA weighted round robin)
- Spill over
  - Use 1 WAN until a specific traffic level is reached then send excess to next Wan
- Source-Destination IP
  - Hash based on source AND destination IP
  - Same source to a different IP will use a different WAN interface
- Measure Volume (?)
  - Maintains a traffic ration between all Wan links
  - Eg: Wan1 has ration 2, Wan2 has Ratio 3 … Wan2 will pass 50% more traffic

21

FORTINET

Virtual Wan Link: Link Quality

- Latency based
  - Based purely on packet response time
- Jitter based
  - Based on CHANGES in packet response time
  - QOS requires predictability in the network traffic

	Wan 1	Wan 2	Jitter	
			Wan 1	Wan 2
Ping #1	1 ms	4 ms	0	0
Ping #2	3 ms	4 ms	2	0
Ping #3	1 ms	3 ms	2	1
Ping #4	3 ms	4 ms	2	1

22

FORTINET

Virtual Wan Link

- Multiple interfaces can be added to the Virtual Wan link
  - » Minimum 1
  - » Interfaces can be any mode (DHCP, etc)

DF bit Support: What is it?

- DF is a one of the flags on a packet that indicates that the packet should not be fragmented, if it is set.
  - » Configure the FortiGate to honor the DF bit or not
- Why not just honor the DF bit all the time?
  - » PPPOE (MTU of 1492)
  - » L2TP (MTU of 1460)
  - » GRE (MTU of 1476)
  - » Tunnel like IPSEC (MTU variable depending on proto/ encapsulation ~1400)
  - » Packets larger then the MTU can not be sent and either need to be fragmented or are dropped.

DF bit Support: Configuration

- Honor DF setting, or not

```
config sys global
     set honor-df [enable|disable]        ; default is enable
end
```

- This effects the behavior of the path mtu setting
  - » Automatic MTU discovery

```
config sys global
     set send-pmtu-icmp [enable|disable]  ;   default is enable
end
```

- When honor-df is set to disable, no imcp messages will be sent
  - » PMTU discovery will break

25 FORTINET

Last Login time: Record last time admin users logged in

- Behavior to store the last login is configurable

```
config sys global
       set login-timestamp [enable|disable]  ; default is disable
end
```

- If enabled, information will be stored in the config file

```
config login-time
       edit "(admin_username)"
              set last-login (date & time)
              set last-failed-login (date & time)
       end
```

26 FORTINET

Combining Proxy and Flow based inspection

- This has never been a good idea, or a recommended configuration
  - » Flow examines traffic as a stream
  - » Proxy changes the traffic
- 5.4 may see some checks in order to prevent this sort of configuration
  - » Possibly warnings about it in the GUI/CLI
- if Flow and Proxy inspection are combined in the same policy, all inspection will be silently converted to Proxy.

Configured	Resulting Inspection
Flow AV & Proxy Web Filter	Proxy AV & Proxy Web Filer
Proxy AV & Flow Web Filter	Proxy AV & Proxy Web Filer

27

FORTINET

FORTINET TRAINING SERVICES

VOIP: New Features & Changes

- Default behavior change for SIP
- Configurable default for handling SIP

Default Behavior Change for SIP

Previous versions of FortiOS used the SIP session helper for all SIP sessions. You had to remove the SIP session helper from the configuration for SIP traffic to use the SIP ALG.

ALG - Application-level gateway (SIP Proxy)

Now, by default all SIP traffic is processed by the SIP ALG (VoIP profile on the firewall policy or not)

Configurable default for handling SIP

```
config system settings
      set default-voip-alg-mode {proxy-based | kernel-helper-based}
end
```

- If SIP traffic is accept by a Firewall policy with a VOIP profile, ALG is used regardless of `default-voip-alg-mode` setting
- If SIP traffic is accept by a policy without a VOIP profile, `default-voip-alg-mode` setting applies.

31

FORTINET

FORTINET TRAINING SERVICES

Routing: New Features & Changes

- ECMP
- BGP
- OSPF
- IPv6

ECMP

- Have ECMP operate based on destination IP as well
  - » Default ECMP behavior only looks at Source IP

```
config sys setting
    set v4-ecmp-mode ?
end
```

- Only possible if Virtual-Wan-Link is NOT enabled

BGP: Neighbor Groups

- Support added for BGP Neighbor groups
  - » Allows for configuration large # neighbors based on an Address range
- Step1: Add the Group

```
config router bgp
        config neighbor-group
        edit <neighbor-group-name>
                set remote-as 100

        end
```

- Step 2: Add the Range

```
config router bgp
        config neighbor-range
        edit 1
                set prefix 192.168.1.0/24
                set max-neighbor-num 100
                set neighbor-group <neighbor-group-name>
        end
```

35

BGP: Conditional Advertising

- Support added for conditional route advertising
- Previously route advertising was Yes/No (Always advertise, or never advertise).
  - » Support added to advertise route (or not) based on the existence or non-existence of other routes.

36

OSPF

- OSPF fast hello provides a way to allow sending of hello packets in intervals less than one second, thus to support as less as one-second dead intervals.
  - » Dead interval measured in hello packets rather then time.
  - » Enable by setting `dead-interval` to 1.
  - » `hello-multiplier` can be set from CLI to set the number of Hello packets per second (4-10)
- Originally a Cisco feature to allow for faster network convergence.
  - » Devices with different `hello-multipier` values can establish adjacency
  - » Cisco allows for values 3-20

37 FORTINET

IPv6

- Support for RFP (Reverse Path Forward)

Check source address type and route to the source address from the incoming interface. If the source address type is invalid or there is no route to the source address from the incoming interface in the IPv6 routing table, or when strict-src-check is set and the route is not the best, the packet will be dropped.

38 FORTINET

High Availability: New Features & Changes

- Requirements Change
- IPSec VPN negotiation
- HA Management interface
- VRRP
- New CLI commands

Requirements Change

- Support for interfaces with Dynamic IPs on devices in an HA cluster.
  - » DHCP, PPPoE

41

IPSec VPN negotiation

- Support added for RFC 6311

  IKE Message ID sync support allow IKEv2 to re-negotiate send and receive message ID counters after HA fail over

- Allows for proper IPSecv2 tunnel renegotiation on HA failover.

42

HA Management interface

- Support added for the following, from the HA Management interface
  - » SNMP management
  - » Sending log messages

VRRP

- VRRP Group support added
  - » All VRRP members in the same group track each others state and if 1 changes they will all change

```
config system interface
       edit (port)
       config vrrp
              edit (vrid)
                     set vrgrp (group id)
              next
       end
end
```

New CLI Commands (for HA)

```
diag sys ha set-as-master [enable | disable]
```

- If set to disable, date/time can be specified (optionally)

```
config system ha
      set override enable
      set override-wait-time <time>
end
```

- If override is enabled, master/slave renegotiation happens when device joins cluster (immediately)
- `override-wait-time` Allows for a delay in master slave negotiation

45 FORTINET

End

46 FORTINET